TAMPEREEN
AMMATTIKORKEAKOULU

Lohkoketjun käyttö datan varmentamiseen

Jukka Pajulehto

Opinnäytetyö
Toukokuu 2018
Tieto- ja viestintätekniikka
Ohjelmistotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Ohjelmistotekniikka

PAJULEHTO JUKKA
Lohkoketjun käyttö datan varmentamiseen

Opinnäytetyö 26 sivua
Toukokuu 2018

Opinnäytetyön tarkoituksena on tutkia lohkoketjuteknologiaa ja selvittää kuinka sitä voidaan soveltaa tiedostojen tallentamiseen ja aikaleimaamiseen käyttäen Factom lohkoketjua. Samalla käydään läpi lohkoketjuteknologian mahdollistavia tekijöitä.

Lohkoketju on yksinkertaisesti selitettynä hajautettu, muuttamaton tietokanta. Nämä ominaisuudet saavutetaan käyttäen P2P verkkomallia, kryptografiaa ja peliteoriaa. P2P verkko pitää huolen lohkoketjun hajautuneisuudesta ja kryptografia takaa lohkoketjun rakenteen. Uusien lohkojen luomisesta ja sääntöjen noudattamisesta vastaa konsensus algoritmi, johon on sovellettu peliteoriaa.

Lohkoketju muuttamattoman luonteensa takia soveltuu hyvin virtuaalisten valuuttojen luontiin. Jokainen valuutansiirtotapahtuma voidaan jäljittää valuutan luomishetkestä nykypäivään, mikä takaa sen, että saman valuuttayksikön käyttäminen kahteen kertaan on vaikeaa.

Virtuaalisten valuuttojen lisäksi lohkoketju soveltuu hyvin tärkeiden dokumenttien varmentamiseen. Jokainen lohko sisältää luomishetken aikaleiman, joten lohkoon tallennettu data on sidottu tähän ajanhetkeen. Tämä tekee dokumenttien auditoinneista helppoa, sillä lohkoketjussa on todiste dokumentin olemassaolosta tietyssä muodossa tiettynä ajankohtana.

Factom lohkoketju tarjoaa helpon ja halvan tavan aikaleimata tiedostoja luotettavasti. Hinta yhden kilotavun tallentamiseen on 0.001 dollaria. Yhteen kilotavuun mahtuu täydellisesti dokumentista hajautusalgoritmilla tuotettu tiiviste, joka toimii dokumentin sormenjälkenä. Factom lohkoketju myös ankkuroi tallennetun datan Bitcoin lohkoketjuun, varmistaen sen muuttamattomuuden.

Lohkoketjuteknologia on vielä nuori ja nopeasti kehittyvä ala. Suurin osa lohkoketjuista ja niiden päälle rakennetuista palveluista on vielä kesken. Siitä huolimatta teknologian potentiaali arvon varastointiin ja datan varmentamiseen on kiistämätön.

Asiasanat: lohkoketju, factom, bitcoin, kryptografia, aikaleimaus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Information and Communication Technology
Software engineering

PAJULEHTO JUKKA:
Applications of blockchain technology in data validation

Bachelor's thesis 26 pages
May 2018

The goal of this thesis is to explore the possibilities of blockchain technology and explain how it can be used to store and timestamp data using Factom blockchain. It also explains the key principles that enables the blockchain technology.

Blockchain is simply explained decentralized and immutable database. These qualities are achieved by using P2P networking, cryptography and game theory. P2P network makes sure that blockchain is decentralized and cryptography secures the structure. Consensus algorithm makes sure that every participant plays by same rules and ensures the decentralization of block creation process. This is achieved with smart usage of game theory.

Because of its immutable nature, blockchain makes it possible to create virtual currencies. Every transaction can be validated from the very beginning which makes blockchain based currencies scarce, open and hard to double spend.

In addition to virtual currencies, blockchain makes it possible to store and timestamp data. Every block contains the timestamp of when it was created. Data inside the block gets automatically timestamped because of this. This makes document auditing process much easier because blockchain contains the definite proof of documents existence in certain time.

Factom blockchain offers easy and simple way to timestamp documents reliably. The cost of storing 1 kilobyte is only 0.001 dollars which is more than enough space to store hash of the document. Hash functions as a fingerprint of the document in a compact form. Factom blockchain also anchors its data into Bitcoin blockchain, ensuring its immutability.

Blockchain technology is still quite young and fast growing industry. Most of the blockchains and applications built on top of them are still work in progress. Nevertheless the potential of using blockchains for storing value and timestamping data is undeniable.

Key words: blockchain, factom, bitcoin, cryptography, timestamping

SISÄLLYS

LYHENTEET JA TERMIT

Kryptovaluutta	Kryptografiaan perustuva virtuaalinen valuutta
P2P	Peer to peer
RSA	Rivest-Shamir-Adleman algoritmi
ECDSA	Elliptic curve digital signature algoritmi
Factoid	Factom lohkoketjun päävaluutta
EC	Entry credit. Valuutta, jolla maksetaan datan tallentaminen Factom lohkoketjuun.
SHA256	Secure hashing algorithm. Hajautusalgoritmi, joka tiivistää tiedostot 256 bitin kokoisiksi tiivisteiksi.
PoF	Proof of Work. Työpohjainen konsensusalgoritmi, jota käytetään esimerkiksi Bitcoin lohkoketjussa.
Tokeni	Lohkoketjun päävaluutan lisäksi luotuja valuuttoja.
Entry	Factom lohkoketjun alin rakenne, johon itse data tallennetaan.
JSON-RPC	JSON rakenteella toimiva etäkomentoprotokola
Fiat	Valuutta, jonka arvoa ylläpitää valtiot ja organisaatiot. Esimerkiksi euro ja dollari ovat fiat valuuttoja.
B2B	Business to business

1 JOHDANTO

Tärkeiden dokumenttien ja datan varastointi täysin digitaalisesti ja auditointikelpoisesti on ollut aina ongelmallista. Paperisten dokumenttien väärentäminen on vaikeampaa, mutta varastointi epäkäytännöllistä ja auditointi vaivalloista. Digitaalisten dokumenttien väärentäminen on helppoa tarjolla olevien työkalujen avulla, eikä tallennetun tiedoston alkuperäisyydestä ole minkäänlaisia takeita, ilman monimutkaisia pääsynhallinta- ja kirjanpitojärjestelmiä. Yritykset ja organisaatiot joille kertyy paljon auditoitavaa dataa, joutuvat investoimaan suuria rahasummia tämän tyyppisiin systeemeihin. Lohkoketjuteknologia ja sen tarjoama muuttamattomuus voivat vähentää näitä kuluja merkittävästi hyvin sovellettuna.

Opinnäytetyö käy lävitse kuinka lohkoketju teknologiaa voidaan hyödyntää tiedon luotettavuuden varmentamiseen käyttäen Factom lohkoketjua edullisesti ja helposti. Työ selvittää myös lohkoketju teknologian periaatteet, aiheeseen liittyvää kryptografiaa ja teknologian implementointia palvelinpuolella.

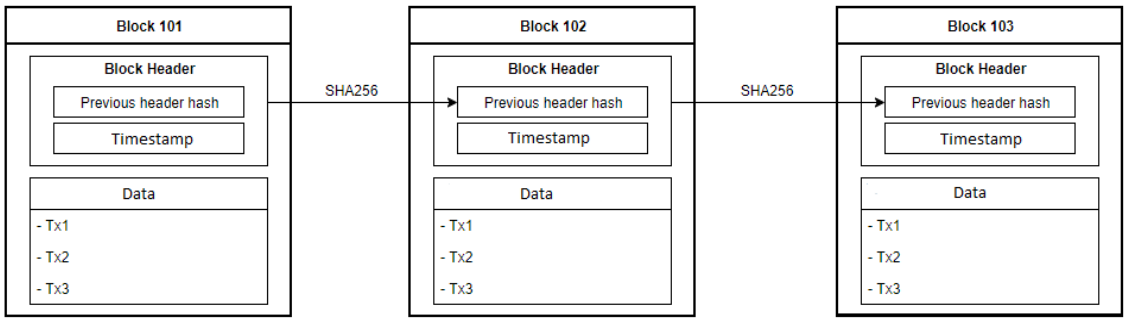
2 MIKÄ ON LOHKOKETJU?

Lohkoketju on yksinkertaisimmillaan selitettynä hajautettu tietokanta, johon tallennettua dataa ei voi muuttaa jälkikäteen. Tallennettu data jaetaan ympäri maailmaa kaikille tietokoneille, jotka ovat osana lohkoketjua. Osallisten välinen kommunikointi ja tiedon jakaminen tapahtuu P2P verkolla. Lohkoketjun rakenne turvataan kryptografialla ja sääntöjen noudattamisen varmistaa konsensus algoritmi, johon on sovellettu peliteoriaa. Näitä lohkoketjun mahdollistavia seikkoja tarkastellaan tarkemmin seuraavissa kappaleissa.

2.1 Lohkoketjun rakenne ja sen turvaaminen

Lohkoketju koostuu kronologisessa aikajärjestyksessä olevista lohkoista, jotka sisältävät dataa (Kuva 1). Nämä lohkot on linkitetty toisiinsa käyttäen hajautusalgoritmeja. Hajautusalgoritmi on algoritmi, joka ottaa vastaan ison tiedoston ja muuttaa sen vakituisen kokoiseksi tiedostoksi. Esimerkiksi SHA256 algoritmi muuttaa kaikki tiedostot 256 bitin kokoisiksi. Hajautusalgoritmeja käyttämällä saadaan ison tiedoston sormenjälki pienennettyä vakituisen kokoisiksi tiivisteiksi. Lohkoketjuissa tätä sovelletaan siten, että uusin lohko sisältää edellisen lohkon header osion tiivisteen. Tämä takaa sen, että lohkoja ei voi muutella jälkikäteen. Jos aikaisempiin lohkoihin tallennettua dataa yritetään muuttaa, muuttuu header osio ja header osiosta laskettu tiiviste. Seurauksena on ketjureaktio, jossa jokainen muutetun lohkon jälkeinen lohko muuttuu myös.

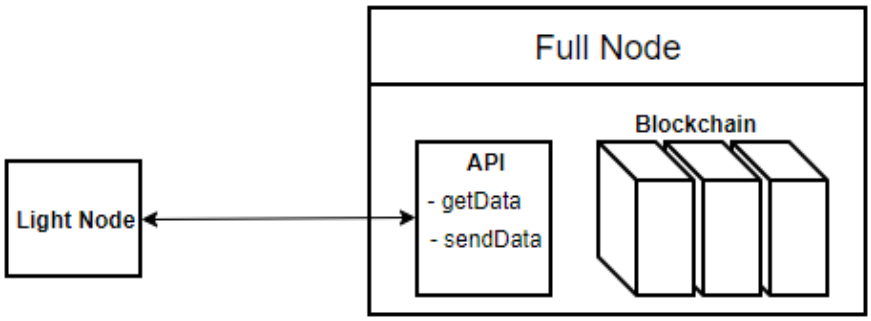
Lohkojen rakenne riippuu paljon lohkoketjusta ja sen käyttökohteesta. Yleensä lohkoista kuitenkin löytyy header ja data osiot. Header osio sisältää lohkoketjun metadataa, kuten lohkon luomishetken ja edellisen lohkon header osion tiivisteen. Data osioon tallennetaan nimen mukaisesti dataa. Bitcoin lohkoketjussa tämä data on allekirjoitettuja valuutansiirtotapahtumia.



KUVA 1. Lohkoketjun rakenne

2.2 Lohkoketjun käyttäminen

Lohkoketjun ja käyttäjän välinen vuorovaikutus vaatii käyttäjäpuolen sovelluksen (Kuva 2). Näitä sovelluksia on kahden tyyppisiä: full node ja light node. Full node sovellus sisältää koko lohkoketjun datan ja mahdollistaa datan tallentamisen, hakemisen ja osallistumisen lohkojen luomiseen. Light node sovellukset hyödyntävät jonkun toisen tarjoamaa full node palvelinta. Eli light node sovellukset lähettävät halutut komennot full node palvelimien käsiteltäväksi. Tällöin täytyy kuitenkin luottaa full node:n tarjoajaan. Light node sovellukset sopivat esimerkiksi mobiililaitteisiin, joissa tallennustila on rajallinen.



KUVA 2. Full node ja light node sovellusten relaatio

2.3 Osallisten välinen kommunikointi

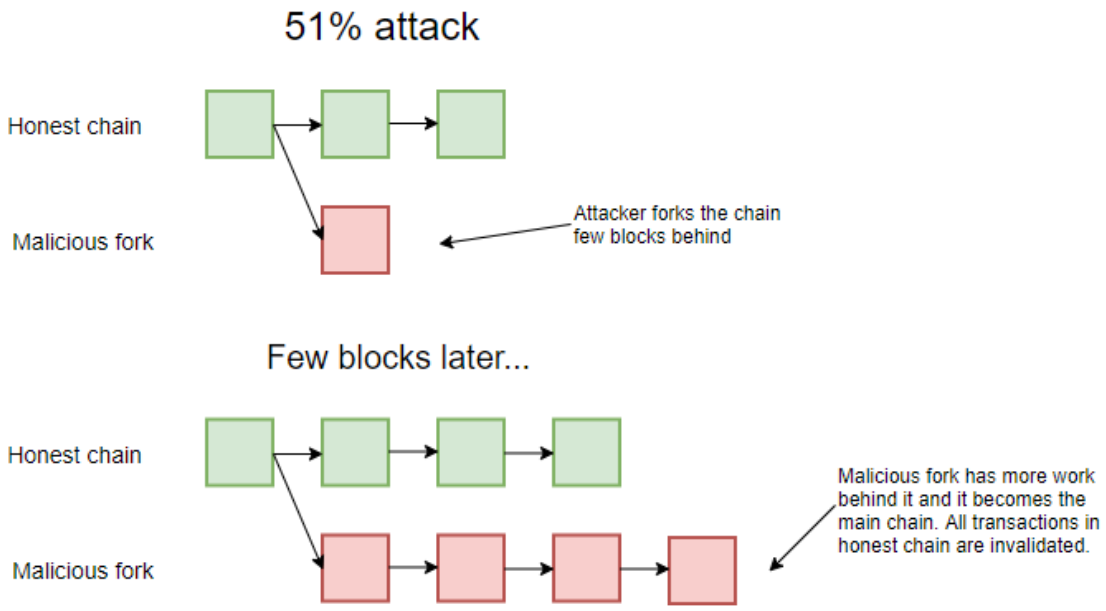
Lohkoketjun osallisten välinen kommunikointi tapahtuu P2P verkkoa käyttäen. Tämä takaa sen, että lohkoketju on mahdollisimman hajautettu ja vaikea sensuroida. Syynä tähän on se, että P2P verkossa laitteet muodosta yhteyden toisiinsa keskittyneen palvelimen sijasta. Jos keskittyneitä palvelimia käytettäisiin, riippuisi lohkoketjun luotettavuus palvelimen ylläpitäjistä.

2.4 Sääntöjen noudattamisen varmistus

Jokaisella lohkoketjulla on omat sääntönsä siitä miten lohkoketjuun tallennettavaksi annettua dataa tulisi käsitellä. Esimerkiksi Bitcoin lohkoketju hyväksyy vain ECDSA secp256k1 käyrästä laskettujen yksityisten avaimien allekirjoituksia (Bitcoinwiki: Secp256k1 2017). Muilla algoritmeilla tuotetut avaimet eivät noudata Bitcoin lohkoketjun sääntöjä, jonka takia ne eivät toimi halutusti. Lohkoketjuun laadittujen säätöjen noudattamisesta ja uusien lohkojen luomisesta vastaa konsensus algoritmi.

Kaikista vanhin konsensusalgoritmi on Bitcoin lohkoketjun käyttämä Proof of Work (Bitcoinwiki: Proof of Work 2016). PoF algoritmin tarkoituksena on hajauttaa uusien lohkojen luomisprosessi monen eri tahon välille tarjoamalla palkinto lohkon luomisesta. Lohkon luominen vaatii kuitenkin ratkaisun vaikeaan matemaattiseen ongelmaan. Tietokoneen laskentatehon nostaminen parantaa mahdollisuuksia voittaa lohkon luomisoikeus ja näin syntyy kilpailua. Kilpailu takaa lohkon luomisprosessin hajautuneisuuden.

Lohkonluomisen hajautuneisuus on tärkeää luotettavuuden kannalta. Jos yksittäinen taho luo yli puolet lohkoista, voi se manipuloida lohkoketjua omiin tarkoituksiinsa. Ilmiötä kutsuttaan 51 % hyökkäykseksi. Bitcoin lohkoketjussa pääketjuna toimii aina ketju johon on käytetty eniten työtä. Yli puolet omistava taho voisi tehdä haaran haluamaan kohtaansa menneisyydessä ja lisätä uuteen ketjuun lohkoja kunnes tästä tulisi pääketju. Mitä pidemmälle menneisyydessä mennään, sitä kauemmin hyökkäyksen toteutus kestäisi. Rehellinen ketju ei pärjäisi, koska tällä on vähemmän laskentatehoa käytössä. Olisi vain ajan kysymys kunnes epärehelliseen ketjuun on käytetty enemmän työtä (Kuva 3).



KUVA 3. 51 % hyökkäyksen mallinnus

PoF algoritmin osalliset tarkastavat myös lohkoon tallennettavan datan oikeudenmukaisuuden. Motiivi tähän on täysin rahallinen, sillä Bitcoin lohkoketjussa rahansiirtotoimenpiteiden tallentamisesta saa myös palkinnon. Lohkojen koko on rajoitettu, joten jokainen viallinen rahansiirtotoimenpide tarkoittaa palkinnon menetystä. Kun lohkon luoja vapauttaa tekemänsä lohkon verkkoon, tarkastaa jokainen osallinen tämän lohkon oikeudenmukaisuuden. Jos lohko on lohkoketjun sääntöjen vastainen, menettää lohkon luoja palkinnon ja lohko hylätään.

Lohkoketjuteknologia soveltaa hyvin peliteoriaa sääntöjen noudattamisen varmistamisessa. Lohkoketju toimii mainiosti niin kauan kun kaikki sen osalliset toimivat rationaalisesti omaa etua ajatellen.

3 LOHKOKETJUN KÄYTTÖKOHTEET

3.1 Virtuaaliset valuutat

Lohkoketjuteknologian ensimmäinen ja suosituin käyttökohde on arvon varastointi ja siirtäminen. Lohkoketjujen avoimuus, sensuroimattomuus ja luotettavuus luovat täydellisen ympäristön arvon varastointiin. Perinteisissä fiat valuutoissa käyttäjät joutuvat luottamaan instituutioihin, kuten pankkeihin. Lohkoketjuun perustuvissa valuutoissa, kryptovaluutoissa, luottamus siirretään ihmisistä kryptografiaan. Tämän takia arvon siirtäminen on halvempaa lohkoketjun välityksellä, erityisesti isojen rahasummien kanssa. Luottamus maksaa ja lohkoketju pystyy eliminoimaan luottamuksen tarpeen. Kryptovaluutoissa on myös ennalta arvattava tai olematon inflaatio, mikä tekee niistä houkuttelevat sijoituskohteen.

Lohkoketjujen muuttamattomuus mahdollistaa kryptovaluuttojen luomisen. Jokainen valuutansiirtotapahtuma voidaan tarkistaa alusta lähtien, jolloin voidaan varmistaa se, että samaa valuuttaa ei ole käytetty useampaan kertaan. Tämä prosessi on kuitenkin työläs lohkoketjun koon kasvaessa, jonka takia valuutansiirtoon suunnitellut lohkoketjut soveltavat merke puita.

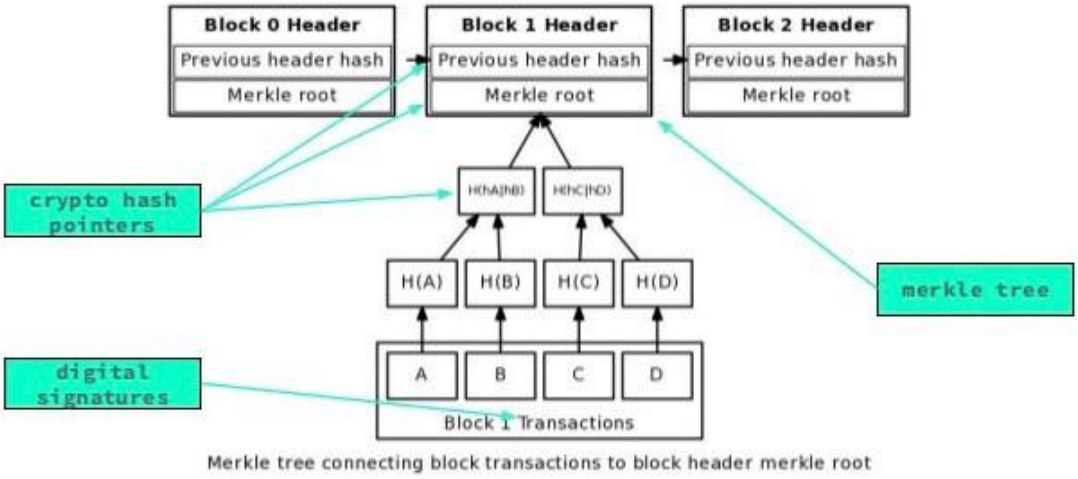
3.1.1 Merke puu

Merkle puu on tiivisteistä koostuva hierarkkinen rakenne (Kuva 4). Rakenteen alinta riviä kutsutaan lehdiksi. Jokainen lehti sisältää tiivisteen. Merkle puu rakennetaan siten, että kaksi tiivistettä liitetään yhteen ja näiden summa laitetaan hajautusalgoritmin lävitse. Tämä toistetaan niin kauan kunnes kaikki lehdet on käsitelty. Jos lehtiä on pariton määrä, summataan pariton lehti itsensä kanssa. Näin päästään ylemmälle tasolle. Tämä metodi toistetaan jokaisella tasolla, kunnes päästään ylimmälle tasolle. Ylin taso sisältää vain yhden tiivisteen, jota kutsutaan Merke juureksi.

Merkle puuta voidaan käyttää datan eheyden nopeaan varmistamiseen. Otetaan esimerkiksi isokokoinen yhden gigatavun tiedosto. Tämä tiedosto voidaan jakaa yhden megatavun kokoisiin osioihin ja nämä osiot taas voidaan muuttaa tiivisteiksi hajautusalgoritmilla. Tällöin meillä on tuhat tiivistettä. Nämä ovat Merkle puun lehtiä. Jos yksikin

näistä megatavun osioista korruptoituu, muuttuu myös tiiviste. Merke puun rakenteen takia tämä heijastuu heti Merkle juuren muuttumisena, mikä tarkoittaa sitä, että tiedosto ei ole alkuperäisessä muodossa. Hierarkkisen rakenteen takia muuttunut megatavun osio voidaan paikantaa ja korvata ilman koko tiedoston uudelleen lataamista. Vain muuttunut osio ladataan uudelleen.

Lohkoketjuissa Merke puuta sovelletaan samalla tavalla mahdollistaen nopean maksutoimenpiteen oikeanmukaisuuden tarkastamisen (Kuva 4). Jos jotain maksutapahtumaan on manipuloitu, muuttuu merke juuren arvo. Muuttunut merkle juuren arvo taas muuttaa lohkon header osiosta lasketun SHA256 tiivisteen ja näin koko lohkoketju muuttuu manipuloidusta lohkosta eteenpäin. Tämän takia lohkoketjun käyttäjien ei tarvitse käydä läpi koko useiden gigatavujen lohkoketjua yhden maksutapahtuman tarkastamiseen.

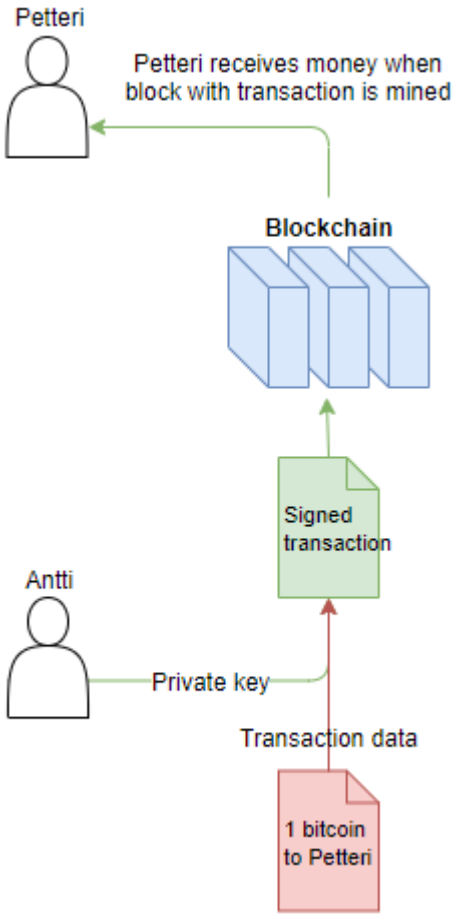


KUVA 4. Merkle puun käyttö lohkoketjuun perustuvissa virtuaalivaluutoissa (Merkle Tree Introduction 2017)

3.1.2 Epäsymmetrisien avainparien käyttö

Epäsymmetrinen kryptografia on toinen tekijöistä, joka mahdollistaa lohkoketju teknologian soveltamisen valuuttojen luomiseen. Epäsymmetrisellä kryptografialla tarkoitetaan julkisen avainparin algoritmeja, joita ovat esimerkiksi RSA ja ECDSA. Näissä algoritmeissa on kaksi osaa: julkinen avain ja yksityinen avain. Yksityisellä avaimella voidaan esimerkiksi salata tiedostoja tai allekirjoittaa digitaalisia dokumentteja. Julkisella avaimella voidaan purkaa vastaavan yksityisen avaimen tekemä salaus tai varmistaa tämän allekirjoittama digitaalinen dokumentti.

Kryptovaluutoissa yksityinen avain vastaa käyttäjän salasanaa ja julkinen avain tiliä. Jos Antti haluaa lähettää valuuttaa Petterille, täytyy tämän tehdä siirtoilmoitus lohkoketjuun. Antti sallii tämän siirron allekirjoittamalla siirtoilmoituksen omalla yksityisellä avaimella. Tämä siirtoilmoitus laitetaan lohkoketjuun, jonka jälkeen siirtotapahtumasta tulee peruuttamaton. Jokainen lohkoketjun käyttäjä voi varmistaa tämän siirtotapahtuman aitouden käyttämällä Antin julkista avainta allekirjoituksen varmistamiseen.



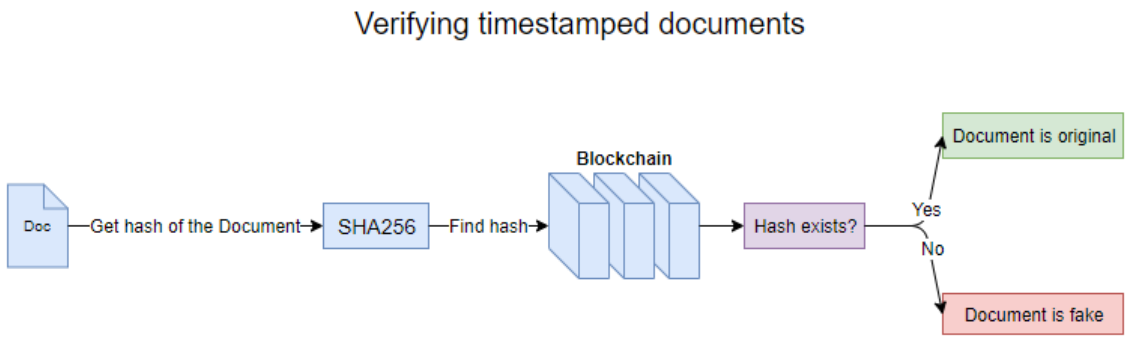
KUVA 5. Antti lähettää Petterille Bitcoin valuuttaa

3.2 Tiedostojen tallentaminen ja aikaleimaaminen

Kuten aiemmin on tullut ilmi, lohkoketjut mahdollistavat arvon varastoinnin ja siirtämisen muuttamattoman luonteensa takia. Tätä ominaisuutta voidaan hyödyntää muihin käyttötarkoituksiin, kuten datan aikaleimaamiseen. Koska kaikki lohkoketjuun tallennettu data säilyy ikuisesti ja jokaisessa lohkossa on aikaleima, soveltuu se datan aikaleimaamiseen ja auditointiin.

3.2.1 Tallennusmenetelmät

Tiedostoja voidaan tallentaa lohkoketjuihin monella eri tapaa, riippuen datan luonteesta. Jos tallennettava data on arkaluonteista, suositeltavana menetelmänä on tiedostojen tallentaminen tiivisteinä. Tämä menetelmä takaa sen, että mikään ulkopuolinen taho ei pysty lukemaan tiedostoja. Tämä myös säästää tilaa lohkoketjussa, sillä tiivisteet ovat aina samanpituisia riippumatta annetun tiedoston koosta. Tiiviste toimii tiedoston sormenjälkenä ja kun tämä sormenjälki tallennetaan lohkoketjuun, saadaan aikaiseksi todiste tiedoston olemassaolosta tietyssä muodossa tiettynä ajanhetkenä. Jos halutaan todistaa jonkin dokumentin alkuperäisyys, laitetaan dokumentti hajautusalgoritmin lävitse ja verrataan saatua tiivistettä lohkoketjuun tallennettuun tiivisteeseen (Kuva 6). Jos nämä täsmäävät, on dokumentti aito. Tämä tekee dokumenttien auditoinnista erittäin helppoa, koska luotto perustuu kryptografiaan ja matematiikkaan.



KUVA 6. Dokumentin alkuperäisyyden varmentaminen

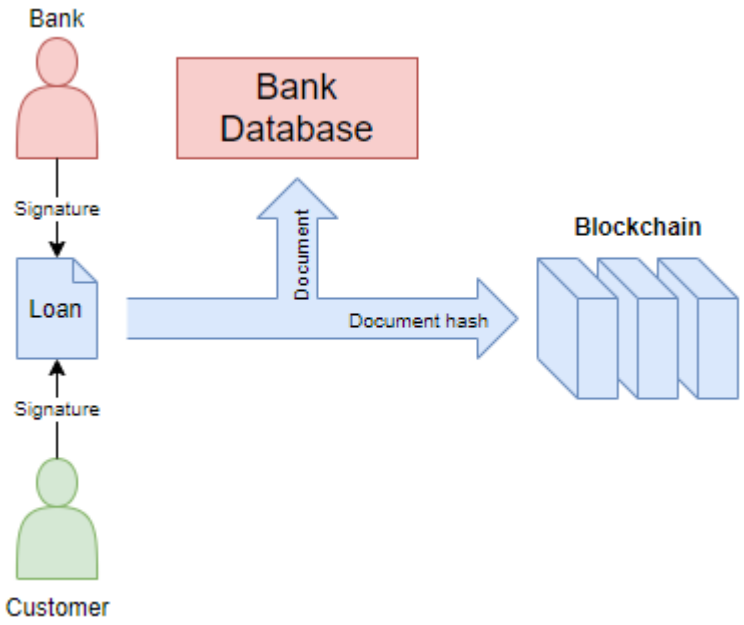
Tiedostot voidaan myös tallentaa salattuna käyttäen esimerkiksi RSA algoritmia. Tämän mallin hyötyinä on se, että alkuperäistä dokumenttia ei tarvitse varastoida. Pelkkä salausavaimen tallentaminen riittää. Tämä ei kuitenkaan ole suositeltava menetelmä muutaman seikan takia. Jos salausavain joutuu vääriin käsiin, on dokumentti kenen tahansa saatavilla ikuisesti. Ajan myötä tietokoneet myös kehittyvät ja esimerkiksi kvanttitietokoneet voivat tehdä joistain salausalgoritmeista hyödyttömiä. Tällöin on vain ajan kysymys kunnes lohkoketjuun tallennettu data paljastuu.

Kolmantena menetelmänä on tiedostojen tallentaminen sellaisenaan. Tämä on tietysti selkein ja helpointapa, jos käsiteltävä data soveltuu siihen koon ja sensitiivisyyden suhteen.

3.2.2 Käytännön sovellutuksia

Suurimman hyödyn lohkoketjujen käytöstä saa alat, joissa syntyy paljon aikaleimaamista vaativaa dataa, kuten sopimusdokumentteja ja kirjautumistietoja. Luontaisesti eniten sovellutus mahdollisuuksia löytyy rahataloussektorista, jossa datan aitouden varmentamiseen ja todistamiseen käytetään huomattavasti resursseja. Lohkoketjuteknologian soveltaminen vähentäisi näitä kuluja huomattavasti, koska aitouden varmistaminen on triviaalia lohkoketjun avulla.

Hyvänä sovellutuskohteena ovat esimerkiksi pankkien tarjoamat lainat (Kuva 7). Käytännössä tämä toteutettaisiin siten, että ensin pankki ja lainanhakija sopivat lainan ehdot. Kun lainan ehdoista ollaan tultu yhteisymmärrykseen ja molemmat osapuolet ovat allekirjoittaneet sopimuksen, laitetaan sopimus tiivisteenä lohkoketjuun. Tällöin kumpikaan osapuoli ei voi muuttaa sopimuksen ehtoja jälkikäteen ilman uuden sopimuksen luomista. Näin pystytään välttämään potentiaalisten oikeusjuttujen syntyminen jo alkutekijöissä.



KUVA 7. Lainasopimuksen aikaleimaaminen lohkoketjuun

Lohkoketjuja voidaan myös soveltaa logistiikka alalla puhtaan datan aikaleimaamiseen. Esimerkiksi ruuan kylmäkuljetukseen voidaan lisätä sensori, joka tallentaa kuljetuksen lämpötilan suoraan lohkoketjuun. Tällöin kuljetusyrityksellä on todiste siitä, ettei kuljetettu ruoka ole rikkonut kylmäketjua. Tällöin myös ravintolalla on todiste siitä, että tarjottu ruoka on käsitelty lainmukaisesti.

3.2.3 Hinta

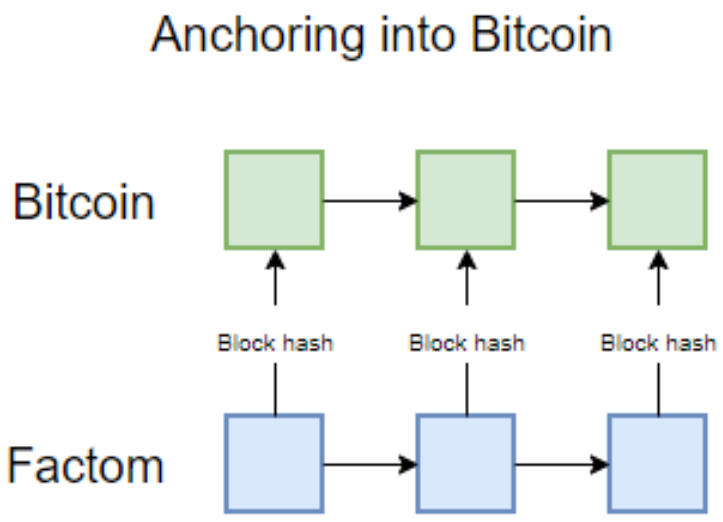
Datan tallentamisen hinta riippuu täysin käytettävästä lohkoketjusta. Jos Bitcoin lohkoketjua käyttäisi edellisen kappaleen esimerkkien tapaan, tulisi aikaleimaamisesta erittäin kallista. Bitcoin lohkoketjua ei kuitenkaan ole suunniteltu tällaiseen käyttötarkoitukseen yhden megatavun lohkojen takia (Block size limit controversy 2018). Tämän takia esimerkkien kaltaiset systeemit vaativat alustakseen jonkun muun lohkoketjun.

4 FACTOM LOHKOKETJU

Factom on lohkoketju, joka on optimoitu ja suunniteltu täysin datan tallentamiseen luotettavasti. Nämä ominaisuuden saavutetaan erilaisella konsensus algoritmilla, kahden tokenin järjestelmällä ja ankkuroinnilla Bitcoin lohkoketjuun. Bitcoin ankkuroinnin takia voidaankin sanoa, että Factom toimii Bitcoin lohkoketjun päälle rakennettuna data kerroksena.

4.1 Ankkurointi

Factom lohkoketju hyödyntää Bitcoin lohkoketjun turvaamiseen käytettyä laskentatehoa ankkuroitumalla siihen. Ankkuroituminen tarkoittaa sitä, että Factom lohkoketjun lohkoja tallennetaan tiivisteinä Bitcoin lohkoketjuun (Kuva 8). Jos joku haluaisi muuttaa Factom lohkoketjuun tallennettua dataa, täytyisi sen myös muuttaa Bitcoin lohkoketjuun tallennettua tiivistettä.



KUVA 8. Factom lohkojen ankkurointi Bitcoin lohkoketjuun

4.2 Konsensus algoritmi

Factom lohkoketjun konsensus menetelmä poikkeaa selkeästi muista lohkoketjuista. PoW:in sijasta Factom käyttää Federated palvelimia (Factom FAQ 2018). Vain Federated palvelimilla on oikeus luoda lohkoja Factom lohkoketjuun. Federated palvelimien ylläpitäjien kesken jaetaan kuukausittain 73 000 Factoidia. Suunnitelmien mukaan Federated

palvelimia olisi kaiken kaikkiaan 33 hajautettuna ympäri maailmaa. Näiden lisäksi konsensus algoritmin osallisina on Audit palvelimet, jotka varmistavat Federated palvelimien toiminnan rehellisyyden. Jos jokin Federated palvelimista käyttäytyy epärehellisesti, korvataan se Audit palvelimella.

4.2.1 Konsensus algoritmin hyödyt ja haitat

Konsensukseen osallistuvien osapuolien vähäinen määrä tarjoaa monia etuja. Koska lohkon kirjoittamisesta annettava palkinto jakautuu vain 33 osapuolen välille, on yksittäiselle taholle annettu palkinto korkea. Korkea palkinto mahdollistaa sen, että Federated palvelimien ylläpitäjät voivat investoida enemmän palvelininfrastruktuuriin, muistiin, prosessointitehoon ja internet yhteyteen. Tämän takia lohkoketjun koko voi olla paljon suurempi aiheuttamatta ongelmia.

Federated palvelinmallilla vältetään myös turhaa resurssien käyttöä. Proof of work menetelmän käyttämä prosessointiteho ja sen kuluttamat resurssit menevät täysin hukkaan. Federated palvelimissa resursseja käytetään niin paljon kuin niitä vaaditaan, eikä turhaa kulua tapahdu.

Federated palvelinten vähäinen lukumäärä on kaksiteräinen miekka. Se tarjoaa tehokkaan ja skaalautuvan konsensusmenetelmän. Tämän hintana on kuitenkin hajautuneisuuden väheneminen, mikä on lohkoketjujen luotettavuuden kulmakivi. Mitä hajautuneempi konsensusmenetelmä on, sitä turvallisempi lohkoketju on. Factom lohkoketjussa tämä seikka on otettu huomioon ankkuroitumalla Bitcoin lohkoketjuun.

4.3 Kahden tokenin järjestelmä

Factom sisältää kaksi eri valuuttaa: Factoid ja EC. EC mahdollistaa datan kirjoittamisen Factom lohkoketjuun. Yksi EC oikeuttaa tallentamaan yhden kilotavun edestä dataa lohkoketjuun. EC:t eivät ole jaollisia ja niille on annettu kiinteä 0.001 dollarin hinta. Ainoa tapa saada EC:jä on polttaa Factoid valuuttaa, minkä takia Factoidien arvo nousee lohkoketjun käytön mukaan. Tämä tarjoaa sijoittajille mahdollisuuden investoida datan varmentamiseen ja helpon budjetoinnin yrityksille, jotka käyttävät lohkoketjua. Yritysten ei tarvitse ottaa huomioon kryptovaluuttojen ailahtelevuutta, koska EC hinta on aina vakio.

4.4 Rakenne

Factom lohkoketjun hierarkiassa ylimmän rakenteen nimi on Directory lohko. Directory lohko sisältää Factom lohkoketjun kolme ensimmäistä aliketjua: Admin-, EC- ja Factoid ketjut. Näitä ei ole eritelty kuvassa 9, koska nämä ketjut eivät ole dokumenttien tallentamisen kannalta oleellisia. Jokaisella näistä ketjuista on kuitenkin kriittinen rooli lohkoketjun toiminnan ja käytön kannalta.

1. Admin ketju sisältää lohkoketjun konsensukselle kriittistä dataa. Tähän dataan kuuluu esimerkiksi lohkon luoneen federated palvelimen allekirjoitus. Kyseistä dataa tarvitaan lohkoketjun rakenteen varmistamiseen.

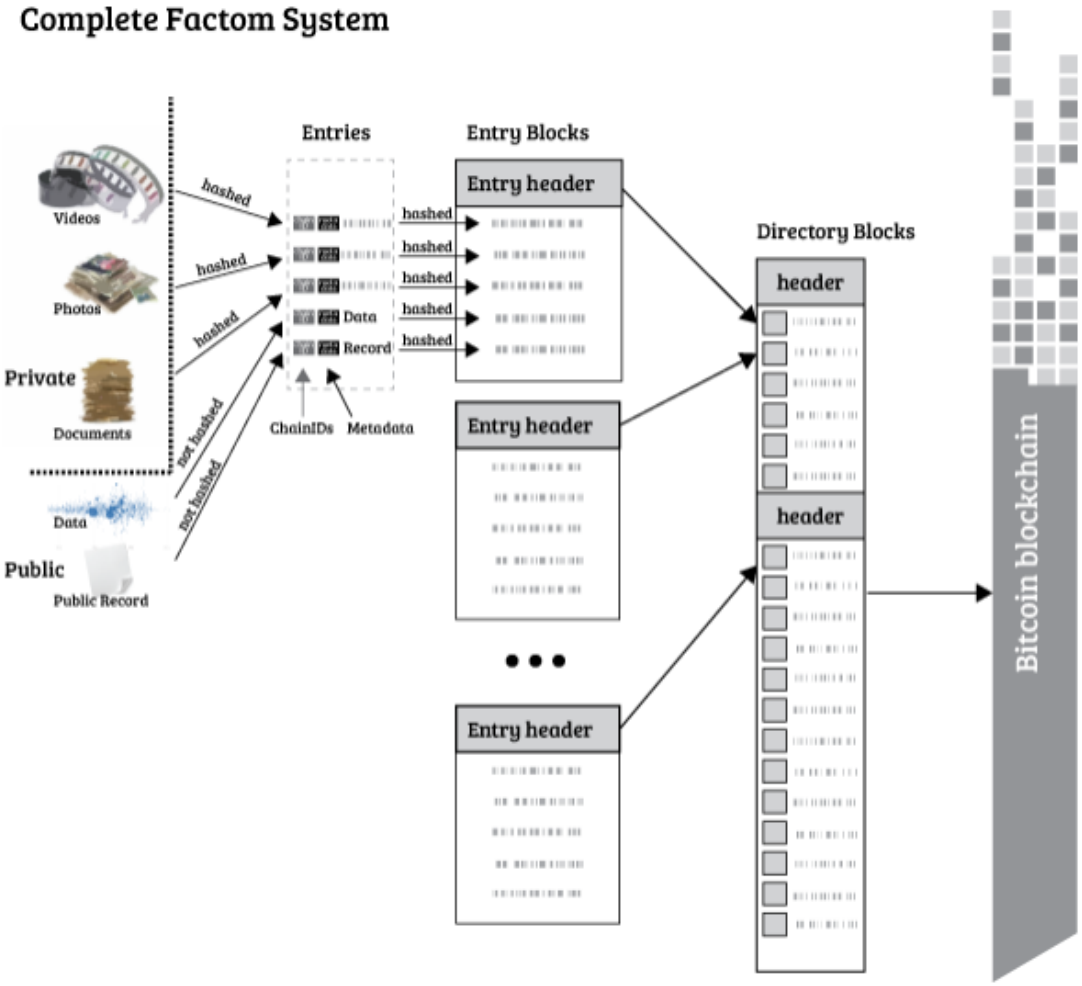
2. Factoid ketjun tehtävänä on pitää kirjaa Factoid valuutan siirtotapahtumista. Tämä ketju toimii melko samalla tavalla kuin Bitcoin lohkoketju.

3. EC ketju pitää kirjaa EC:n käyttötapahtumista. Näitä tapahtumia ovat uusien ketjujen luominen ja datan tallentaminen.

Tämän lisäksi Directory lohko sisältää Entry lohkoja (Kuva 9). Entry lohko on rakenne, joka organisoi käyttäjien luomat entry:t oikeisiin ketjuihin. Entry lohkoon kasataan kaikki entry:t, jotka halutaan tallentaa tiettyyn ketjuun viimeisen kymmenen minuutin aikana.

Entry on hierarkiassa kaikista alin rakenne, joka sisältää Factom lohkoketjuun tallennetun datan.

.



KUVA 9. Factom lohkoketjun rakenteen kokonaiskuva (Factom whitepaper 2014, sivu 15)

5 FACTOM LOHKOKETJUN KÄYTTÄMINEN

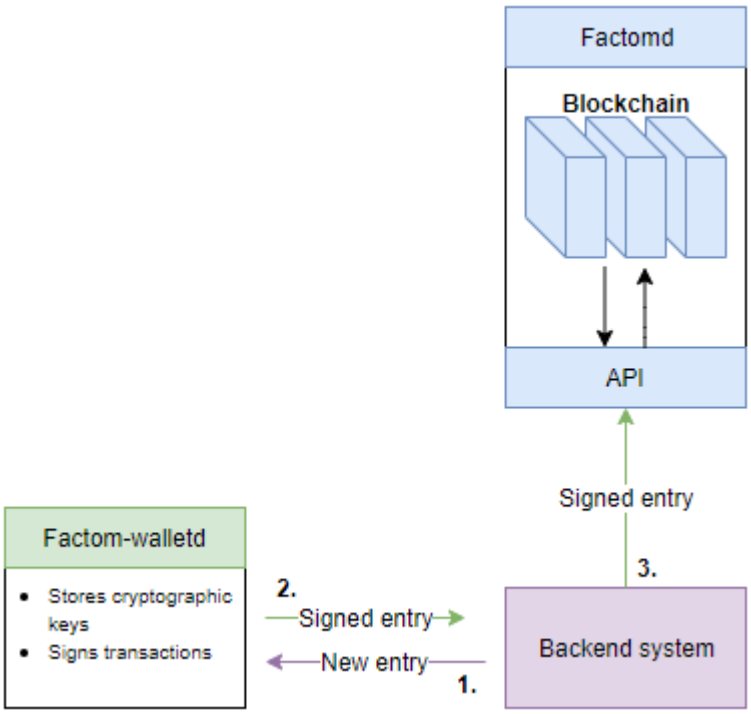
5.1 Vaatimukset

Kuten kappaleessa 2 mainittiin, jokaisen lohkoketjun käyttäminen vaatii yhteyden full node sovellukseen. Factom lohkoketjussa full node sovelluksena toimii factomd taustaprosessi, joka vastaanottaa komentoja käyttäen JSON-RPC protokolaa. JSON-RPC protokola tarkoittaa yksinkertaisesti komentojen lähettämistä etäpalvelimeen JSON muotoa käyttäen. Näin Factom lohkoketjun käyttö on helppoa kaikilla ohjelmointikielillä.

Factom lohkoketjun kryptografisten avainten hallintaan voidaan käyttää factom-walletd ohjelmaa, joka tallentaa avaimet salattuna kovalevylle. Factom-walletd toimii hyvin factomd sovelluksen kanssa, jonka takia tämä on suositeltava menetelmä avaimien varastointiin ja käyttöön. Avaimien tallentamisen voi hoitaa myös itse tilanteen vaatiessa. Tällöin kuitenkin joutuu myös rakentamaan valuutansiirtotapahtumat ja niiden allekirjoittamiset omassa koodissa.

5.2 Arkkitehtuuri

Aina kun Factom lohkoketjuun halutaan lisätä dataa, täytyy siitä maksaa. Maksaminen toteutetaan factom-walletd:n varastoimilla EC avaimilla. Tämän takia tallennettavan datan sisältämä entry täytyy lähettää ensin factom-walletd sovellukselle allekirjoitettavaksi (Kuva 10). Allekirjoitettu entry voidaan tämän jälkeen lähettää factomd sovellukselle, joka hoitaa entry:n tallentamisen lohkoketjuun.



KUVA 10. Tiedon liikkuminen Factom pohjaisessa sovelluksessa

5.3 Esimerkkiprojekti

Esimerkkiprojekti on toteutettu käyttäen JavaScript ohjelmointikieltä ja node.js ohjelmistokehystä. Node.js kehys mahdollistaa JavaScript koodin suorittamisen palvelinpuolella. Syy JavaScript:in valintaan on parempi Factom kirjastojen tarjonta, joka helpottaa lohkoketjun integroimista omiin sovelluksiin.

Npm kirjastonhallintatyökalu tarjoaa Factom nimisen paketin, joka sisältää korkeamman tason toiminnollisuuksia. Näitä toimintoja on esimerkiksi uusien ketjujen luominen, Factoid valuutan lähettäminen ja datan tallentaminen. Kirjasto hoitaa JSON-RPC kommunikoinnin factomd ja factom-walletd sovelluksiin päin käyttäen helppoja funktioita, säästäen aikaa ja vähentäen koodin kompleksisuutta.

Datan tallentaminen ja aikaleimaaminen Factom lohkoketjuun tapahtuu sovelluskohtaisten ketjujen muodossa. Jokainen Factom lohkoketjua hyödyntävä sovellus voi luoda yhden tai useamman ketjun omiin käyttötarkoituksiinsa. Alla olevassa koodissa (Kuva 11) rivillä 17 luodaan nuolifunktio, jonka tehtävänä on luoda testiketju. Uuden ketjun luominen vaatii myös yhden entry:n luomisen. Tähän voidaan tallentaa esimerkiksi ketjun tarkoitus. Entry:n luominen tapahtuu helposti käyttäen Factom kirjaston tarjoamaa Entry

luokkaa. Entry luokan rakentajalle annetaan parametreiksi tallennettava data ja tämän muoto. Tämän jälkeen luotu entry olio annetaan chain luokan rakentajalle parametriksi. Valmis chain olio ja entry credit osoite annetaan factomd sovellukselle, joka hoitaa uuden ketjun luomisprosessin. Tämä voi kestää maksimissaan 10 minuuttia, koska Factom lohkoketju ankkuroituu Bitcoin lohkoketjuun 10 minuutin välein.

```
1  const {FactomCli,Entry,Chain} = require("factom")
2  const crypto = require("crypto-js")
3
4  ecAddress = "EC3SYqEfuT9iHJ9nS8H87BQy4AVtLHozY3Vqz9zgbVSUr5T77C4i"
5
6  const client = new FactomCli({
7      factomd:{
8          host:"courtesy-node.factom.com",
9          port:80
10     },
11     walletd:{
12         host:"localhost",
13         port:8089
14     }
15 })
16
17 var createNewChain = () =>{
18     var entry = Entry.builder()
19         .extId("EpicTestChain","utf8")
20         .content("This chain is for testing purposes!","utf8")
21         .build()
22     var chain = new Chain(entry)
23     client.addChain(chain,ecAddress)
24 }
25
26 var createNewEntry = () =>{
27     var document = "important file"
28     hashedDocument = crypto.SHA256(document).toString()
29     var entry = Entry.builder()
30         .chainId("8ab5c09369067909bffd5e1246042dcc6ee6584b9a6a0e2153de9863f80eeae6")
31         .extId("Document 1","utf8")
32         .content(hashedDocument,"utf8")
33         .build()
34     client.addEntry(entry,ecAddress)
35 }
36
37 createNewEntry()
38
```

KUVA 11. Uuden ketjun luominen ja esimerkkidatan tallentaminen

Kun ketju on luotu, voidaan siihen tallentaa dataa. Rivillä 26 on nuolifunktio, joka tallentaa esimerkkidatan tiivisteen esimerkkiketjuun. Rivillä 28 esimerkkidata laitetaan SHA256 hajautusalgoritmin lävitse, jolloin saadaan 256 bitin kokoinen tiiviste. Tämän jälkeen luodaan entry olio, jolle annetaan parametreiksi ketjun id ja tallennettava tiiviste.

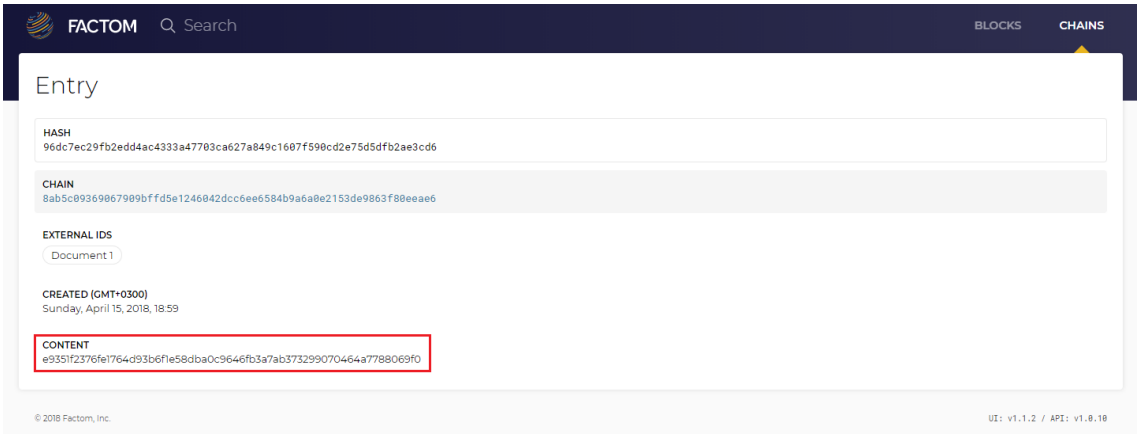
Ketjun id johdetaan alla olevasta kaavasta (Kaava 1), jossa ”extId” tarkoittaa ketjun nimiä ja ”n” tarkoittaa ketjun nimien lukumäärää aloittaen indeksistä 0.

$$Chain\ Id = SHA256(SHA256(extId[0]) + SHA256(extId[1]) + \cdots + SHA256(extId[n]))$$

KAAVA 1. Ketjun Id:n laskeminen (Factom Data Structures 2018)

Valmis entry olio annetaan samaan tapaan kuin ketjua luodessa factomd sovellukselle prosessoitavaksi ja 10 minuutin päästä esimerkkitiedoston sormenjälki on aikaleimattu Factom lohkoketjuun ikuisesti.

Lohkoketjun sisältämää dataa voidaan tarkastella esimerkiksi explorer.factom.com sivun välityksellä. Sivusto tarjoaa graafisen käyttöliittymän tallennetun datan tarkastelemiseen ilman omaa full node sovellusta. Alla olevassa kuvassa näkyy (Kuva 12) kuinka esimerkkitiedosto on tallentunut testiketjuun onnistuneesti.



KUVA 12. Esimerkkidatan SHA256 tiiviste Factom explorer sivustossa

5.4 Huomion arvoisia seikkoja

Factom lohkoketjussa kuka tahansa voi tallentaa dataa mihin tahansa ketjuun. Tämän takia tallennetun datan validointi täytyy tapahtua omassa sovelluksessa jos käyttökohde sitä vaatii. Tämä voidaan esimerkiksi toteuttaa siten, että tallennettava data allekirjoitetaan käyttäen ECDSA avainparia. Tällöin on helppo erotella mikä lohkoketjuun tallennetusta datasta on sovelluksen tallentamaa ja mikä ulkopuolisten tahojen.

6 POHDINTA

Vaikka idea kryptografiaan perustuvista valuutoista on pyörinyt 1990-luvulta lähtien, on lohkoketju teknologiana vielä melko nuori (Before Bitcoin Pt.2 2018). Bitcoin vanhimpana lohkoketjunakin on vain 9 vuotta vanha. Suurin osa kehitteillä olevista lohkoketjuista ja näiden päälle rakennetuista sovelluksista on vielä kesken. Lohkoketjuteknologian potentiaali on kuitenkin kiistämätön ja monet eri talouden sektorit tulevat hyötymään sen soveltamisesta. Ethereum lohkoketjun tarjoama tokenien luonti ja älykkäät sopimukset ovat jo mullistaneet startup yritysten rahoittamisen. Samat tokenit mahdollistavat fyysisten omaisuuden, kuten kullan ja kiinteistöjen, virtualisoinnin. Tulevaisuudessa voi olla hyvinkin mahdollista, että kaikki omaisuus, olkoon se digitaalista tai fyysistä, keskittyy lohkoketjuihin kaupankäyntiä varten.

Lohkoketjuteknologian käyttäminen dokumenttien aikaleimaamiseen on toinen kryptovaluuttojen ja tokenien varjoon jäänyt sovellutuskohde. Syinä tähän on se, että dokumenttien aikaleimaaminen lohkoketjuun on melko paljolti B2B ratkaisu, eikä se kosketa yksittäisiä ihmisiä suoraan. Parhaassa tapauksessa lohkoketjuun aikaleimaamista soveltavan yrityksen, kuten pankin, asiakkaat eivät edes tiedä, että lohkoketjua käytettiin asuntolainasopimuksen aikaleimaamiseen. Suurimman hyödyn aikaleimaamisesta saa myös isot ja vakiintuneet yritykset, joille kertyy paljon tärkeää, auditointia vaativaa dataa. Loppuen lopuksi lohkoketjun käyttämisestä seuraava riskitekijöiden aleneminen kuitenkin heijastuu käyttäjille halvempien hintojen muodossa.

LÄHTEET

Evan Kozliner. 27.9.2017. Merkle Tree Introduction. Luettu 20.5.2018. https://medium.com/@evankozliner/merkle-tree-introduction-4c44250e2da7

Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby. 17.11.2014. Factom whitepaper. Luettu 18.5.2018. https://github.com/FactomProject/FactomDocs/raw/master/Factom_Whitepaper.pdf

Bitcoinwiki. Päivitetty 5.5.2018. Block size limit controversy. Luettu 19.5.2018. https://en.bitcoin.it/wiki/Block_size_limit_controversy

Pet3rpan. 4.4.2018. Before Bitcoin Pt.2 Luettu 19.5.2018. https://medium.com/bitfwd/history-of-things-before-bitcoin-cryptocurrency-part-two-94c4576005

Factom. Factom Data structures. Luettu 17.5.2018. https://www.factom.com/devs/docs/guide/factom-data-structures

Bitcoinwiki. Päivitetty 23.12.2017. Secp256k1. Luettu 19.5.2018. https://en.bitcoin.it/wiki/Secp256k1

Bitcoinwiki. Päivitetty 15.5.2016. Proof of work. Luettu 19.5.2018. https://en.bitcoin.it/wiki/Proof_of_work

Factom. Factom FAQ. Luettu 18.5.2018. https://www.factom.com/about/faqs